

OPTOS PRIVACY NOTICE

In this privacy notice we explain how we collect and use your personal data. This privacy notice applies to all personal data we process about you when you order, purchase or use our products and services, visit our websites, use our customer support or otherwise interact with Optos plc.

Optos plc respects privacy and acknowledges that processing personal data in a lawful and proper manner is an important social responsibility and declares that it will strive to protect personal data. As such we are providing this privacy notice as part of Nikon's Group Privacy Protection Statement <url: www.nikon.co.jp/main/eng/privacy_policy.htm> and applies to all personal data that we process concerning our prospective, current and former customers and suppliers (hereafter "you"), and your usage of our products and services, our Optos website at <https://www.optos.com/>, or otherwise doing business with Optos plc. In this privacy notice, we explain which personal data we collect and how we use this data. Therefore, we encourage you to read this notice carefully.

Contents

- 1. Who we are**
- 2. What personal data we collect and what we do with your data**
- 3. How we collect your data**
- 4. Information sharing**
- 5. Security measures and data retention**
- 6. International transfers of personal data**
- 7. Your rights**
- 8. How we look after this policy**
- 9. Contact details for your privacy inquiries**

Policy P-SP130-5

1. Who we are

We are Optos. References within this notice to “Optos” include Optos plc, Queensferry House, Carnegie Campus, Dunfermline, Scotland KY11 8GR United Kingdom, and Optos inc, 500 Nickerson Road, Suite 201, Marlborough, MA 01752, USA. Both are part of the Nikon Group. Together with Nikon Corporation, Shinagawa Intercity Tower C, 2-15-3, Konan, Minato-ku, Tokyo, 108-6290, Japan, we are responsible for the collection and use of your personal data described in this privacy notice. References to “**Nikon**”, “**Optos**”, “**we**” and “**our**” throughout this notice, depending on the context, collectively refer to the aforementioned legal entities.

Optos is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice. The legislation that we adhere to is as follows: United Kingdom General Data Protection Regulation (UK GDPR), EU General Data Protection Regulation 2016/679 (EU GDPR) and the Data Protection Act 2018. Optos’ leadership is fully committed to ensuring continued and effective compliance with this legislation and the implementation of all aspects of this Notice. This includes providing all staff with adequate training on data protection requirements backed up where necessary by internal and external auditing. Furthermore, all staff are made aware that failure to adhere to data protection principles may result in internal disciplinary action.

If you are a California consumer within the meaning of the California Consumer Privacy Act of 2018 (“CCPA”), please refer to this notice alongside our CCPA addendum- [optos.com/globalassets/public/optos/corporate-information/ccpa-privacy-policy-form-addendum-optos.pdf/](https://optos.com/globalassets/public/optos/corporate-information/ccpa-privacy-policy-form-addendum-optos.pdf)

We have determined our respective responsibilities for compliance with the obligations under applicable privacy legislation for processing your personal data in relation to our global processing activities by means of an arrangement between us. In summary, we have arranged that if you want to exercise your rights, such as your right to access, correct, erase, restrict, object or port personal data or to withdraw your consent, or if you have any questions about the processing of your personal data, you can contact Optos in accordance with Section 9 of this notice below. Optos and Nikon Corporation will assist each other where necessary to ensure that you can exercise your rights and that your questions will be handled.

2. What personal data we collect and what we do with your data

We have outlined our data processing operations and the purposes for which we process your personal data in the Overview of Optos processing activities in the Annex below. In summary, we use various systems to deliver products and services

to you. For example, Optos provide the following products and services: Scanning Laser Ophthalmoscopes, Optical Coherence Tomography Systems, Picture Archiving and Communication Software, Customer Service Support, Pre-Sales Business Development and Marketing and Post Marketing Device Support.

Special Category Data

Some of the personal data described in the Overview in the Annex below may be considered to be “special category data”, or “sensitive personal information” under applicable data protection laws. For example, health and medical data and/or biometric data including the retinal image and ethnicity of a patient may qualify as sensitive data.

Optos will only process these data in accordance with applicable data protection laws. As such, processing of these data is not undertaken without first identifying the lawful basis, and the subsequent “condition of processing” also. For example, “medical data” will be processed either under the lawful basis of contract or legal obligation, with the condition of processing identified as “explicit consent” or “necessary for medical diagnosis or preventative medicine”.

We have outlined these data in the Overview of Optos processing activities below.

Lawful basis

Optos processes your personal data to provide our products and services to you, to comply with legal obligations to which we are subject, if it is necessary for our legitimate interests or the interests of a third party, or on the basis of consent. See Annex below for indicative examples of our data processing and the lawful bases upon which we rely. We recognise that more than one lawful basis cannot be used for a single processing activity. However, for the purposes of this Notice, certain processes have been amalgamated for brevity.

When we process your personal data for our legitimate interests or the interests of a third party, we will take reasonable measures to prevent unwarranted harm to you. We will also carry out a ‘balancing exercise’ to ensure that our interests do not outweigh those of the data subject. Our legitimate interests are for example, our interest of improving our product and services delivery by storing contact details, reducing our costs, improving our newsletters and websites by analysing which parts of our communications are most relevant for you. Or of securing our services and facilities, such as the purposes mentioned in the Annex. More information on the balancing tests we perform is available upon request. Where we process your personal data for our legitimate interests or the interests of a third party, you have the right to object at any time on grounds relating to your particular situation (please see Section 7 below).

You may withdraw your consent at any time by following the specific instructions in relation to the processing for which you provided your consent, by adjusting your setting (if available) or by reaching us through the contact details in Section 9 below.

Where we process your personal data for a purpose other than that for which we collected it initially (and we rely on a legal basis other than consent or complying with legal obligations for this new purpose), we will ascertain whether processing for this new purpose is compatible with the purpose for which the personal data were initially collected. More information on this assessment is available upon request (please see Section 7 below).

In relation to processing your special category personal information and why we process your medical information is because (1) you have provided your explicit consent, (2) to carry out our legal obligations, (3) it is necessary for the establishment, exercise or defence of legal claims, (4) it is needed for reasons of substantial public interest, such as for equal opportunities monitoring.

3. How we collect your data

Most of the personal data we process is information that you knowingly provide to us directly or through third parties. However, in some instances, we process personal data that we are able to infer about you based on other information you provide to us or on our interactions with you, or personal data about you that we receive from a group company or a third party with or without your knowledge (please see Section 4 and the Annex below).

If you refuse to provide personal data that we require for the performance of a contract or compliance with a legal obligation, we may not be able to provide all or parts of the services you have requested from us.

4. Information sharing

Optos, and its subsidiaries, will process some of your personal data locally. However, as a global organization, many of our business activities can also be carried out by processing or consolidating information about you in specific or centralized databases and systems located at specific secured facilities worldwide. As a result, your information may be shared with other entities within the Nikon Group. However, each Nikon Group company and those other systems and databases will only collect, receive, use, share or otherwise process such personal data in accordance with applicable laws, this privacy notice, our Nikon Group Privacy Protection Statement <url: www.nikon.co.jp/main/eng/privacy_policy.htm>. Moreover, internally we maintain a strict access policy with regard to the processing

of personal data. Only a limited group of authorized Nikon staff on a need-to-know basis may have access to your personal data.

As a rule, we do not share your personal data with anyone outside the Nikon Group. However, we may share your personal data with trusted third parties that perform business functions or provide services to us. Examples are cloud-based databases, external auditors, and Regulatory Bodies. All such third parties will be required to adequately safeguard your personal data, subject to agreements that correspond to the requirements of applicable laws. Your personal data may also be shared for investigations, and background checks (e.g. disclosure to prevent crime or fraud, or to comply with a court order or legislation). Where trusted third parties are used we will ensure that the contracts between the parties contain all relevant information and assurances to ensure compliance with data protection legislation (Article 28 of UK/EU GDPR).

5. Security measures and data retention

Optos will secure your personal data in accordance with our IT and security policies so that personal data are protected against unauthorized use, unauthorized access and wrongful modifications, loss or destruction. Your personal data will be stored no longer than is necessary for the purpose for which they were obtained, including compliance with legal and fiscal obligations, and for solving any contractual disputes. We have outlined the specific data retention periods in the Overview of Optos processing activities in the Annex below.

6. International transfers of personal data

Given the global nature of our company, your personal data may be transferred to Nikon entities and trusted third parties in countries outside the European Economic Area whose laws may not afford the same level of protection of your personal data, specifically the United States. Where necessary, Optos will ensure that adequate safeguards are in place to comply with the requirements for the international transfer of personal data under applicable privacy laws. For transfers of personal data outside the European Economic Area, Optos will use Commission approved mechanisms, such as the EU-US Data Privacy Framework ('DPF'). Where a third party is not part of the DPF, Optos will revert to other approved mechanisms, namely Standard Contractual Clauses as safeguards, such as the "(EU-)controller to (Non-EU/EEA-) controller" Decision 2004/915//EC (see Article 46 UK/ EU GDPR). If you wish to receive a copy of these safeguards, or obtain more detail about them, please contact us through the contact details in Section 9 below.

7. Your Rights

You can contact us (please see Section 9 below) to exercise any of the rights you are granted under applicable data protection laws, which includes (1) the right to access your data, (2) to rectify them, (3) to erase them, (4) to restrict the processing of your data, (5) the right to receiving a file of your personal data and (6) or the right to object to the processing, and where we have asked for your consent, to withdraw this consent. These rights will be limited in some situations. We will, for example, deny your request for access when necessary to protect the rights and freedoms of other individuals or refuse to delete your personal data in case the processing of such data is necessary for compliance with legal obligations. The right to data portability, for example, does not apply in case the personal data was not provided by you or if we process the data not on the basis of your consent or for the performance of a contract.

When you would like to exercise your rights, please send your request to the contact details in Section 9 below. Please note that we may need you to provide additional information to confirm your identity. You also have the right to lodge a complaint with the Information Commissioner's Office.

You can also contact us at if you have any questions, remarks or complaints in relation to this privacy notice.

7.1. Right to access

You may ask us whether or not we process any of your personal data and, if so, receive access to that data in the form of a copy. You are entitled to this Right of Access regardless of the lawful basis upon which we process your data. When complying with an access request, we will also provide you with additional information, such as the purposes of the processing, the categories of personal data concerned as well as any other information necessary for you to exercise the essence of this right.

7.2. Right to rectification

We are committed to ensuring that the information we hold about you is accurate. However you have the right, regardless of the lawful basis used, to have your data rectified in case of inaccuracy or incompleteness. Upon request, we will correct inaccurate personal data about you and, taking into account the purposes of the processing, complete incomplete personal data, which may include the provision of a supplementary statement.

7.3. Right to erasure

You also have the right to have your personal data erased, which means the deletion of your data by us and, where possible, any other controller to whom your data has previously been made public by us. Erasure of your personal data can only take place in certain cases, prescribed by law and listed under Article 17 of UK/ EU GDPR. Essentially, this means that we will not be able to undertake an erasure request if we are required to hold your data, by law, for a defined period of time, or if it remains necessary for the completion of a contract with you.

The right of erasure includes situations where your personal data are no longer necessary in relation to the initial purposes for which they were processed as well as situations where they were processed unlawfully. Due to the way we maintain certain services, it may take some time before backup copies are erased.

7.4. Right to restriction of processing

You have the right to obtain the restriction of the processing of your personal data, which means that we suspend the processing of your data for a certain period of time. Circumstances which may give rise to this right include situations where the accuracy of your personal data was contested but some time is needed for us to verify the (in)accuracy. This right does not prevent us from continue storing your personal data. We will inform you before the restriction is lifted. We cannot restrict the processing of personal data if the lawful basis upon which we rely is legal obligation, or in order to complete a contract with you.

7.5. Right to receive your file (data portability)

Your right to data portability entails that you may request us to provide you with your personal data in a structured, commonly used and machine-readable format and to have such data transmitted directly to another controller, where technically feasible. Upon request and where this is technically feasible, we will transmit your personal data directly to the other controller.

7.6. Right to object

You also have the right to object to the processing of your personal data, which means you may request us to no longer process your personal data. This only applies in case the 'legitimate interests' ground (including profiling) constitutes the legal basis for processing (see par. 'Lawful basis' above).

At any time and free of charge you can object to direct marketing in case your personal data are processed for such purposes, which includes profiling you to the

extent that it is related to such direct marketing. In case you exercise this right, we will no longer process your personal data for such purposes.

8. How we look after this policy

We have most recently updated this notice on 28 August 2024 and it replaces earlier versions. We will update this privacy notice from time to time and notify you of any substantive changes.

9. Contact details for your privacy inquiries

Optos plc Compliance Department
Queensferry House, Carnegie Campus, Dunfermline, Scotland KY11 8GR United Kingdom
dpo@optos.com
Telephone: +44 (0)1383 843350

Optos inc
500 Nickerson Road, Suite 201, Marlborough, MA 01752, USA
ics@optos.com
Telephone: Toll-free: [800-854-3039](tel:800-854-3039) or [833-655-1770](tel:833-655-1770)

Data Protection Officer:
The DPO Center Ltd, 50 Liverpool Street, London, EC2M 7PY,
dpo@optos.com
[Telephone: +44 \(0\)203 7976340](tel:+44(0)2037976340)

EU Representative:
[The DPO Centre \(Europe\) Ltd](#), Alexandra House, 3 Ballsbridge Park, Dublin, D04 C7H2, Ireland
dpo@optos.com
[Telephone: +353 1 631 9460](tel:+35316319460)

Alternatively, you can manage the communications that you would like to receive from Optos here: <https://www.optos.com/en/landing-pages/manage-your-email-preferences/>

Or unsubscribe from communications here:
<https://www.optos.com/en/landing-pages/unsubscribe/>

OVERVIEW OF OPTOS PROCESSING ACTIVITIES

Processing operation	Categories of personal data	Special categories of personal data	Purposes	Recipients	Retention period	Lawful Basis
Customer Service/ Repair Administration	Address, Country, Email, Location data, Name, Postal Code, Phone number, IP Address	Health and Medical	Patient data can be visible or retained on device during service or replacement process	Service Providers	Life of Device + 2 years	Contract
End Customer Administration	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address	N/A	Customer relationship:	Regulatory Auditors, Supplier Correspondence	Life of Device + 2 years	Contract
Customer Service/ Repair Administration	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address	N/A	Administration, Compliance with law, Customer relationship, Regulatory Reporting	Food & Drug Administration (FDA - US) Medicines & Healthcare Products Healthcare Agency (MHRA - UK) Ministry of Health, Labour and Welfare (MHLW – Japan) Health Canada All other relevant Regulatory Bodies	Life of Device + 2 years	Contract Legal obligation

Vendor Administration	Address, Country, Email, Location data, Postal Code/ Zip code, Name, Phone number, IP Address	N/A	Administration, Compliance with law, Customer relationship, Contract execution, Vendor Management:	Authorized Employees Regulatory Auditors,	Life of Device + 2 Years	Contract Legal obligation
Others Prospective Customer Data	Address, Country, Email, Location data, Postal Code, Name, Phone number, CET Numbers, NPI Numbers, Buying group data, marketing communications and responses, regional demographic data, IP Address	N/A	Direct Marketing, compliance with the law, contract execution	Regulatory Auditors, Transferred to external 3rd party servers	CET - 7 Years/Rest Life of Device + 2 years or life of contract +2 years	Legitimate Interest Legal obligation Contract
Others Distributor Administration	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address	N/A	Direct Marketing, Administration, Customer relationship, Vendor Management:	Regulatory Auditors	Life of Device + 2 years or life of contract +2 years	Legitimate Interest Contract
End Customer Administration	Address, Email, Country, IP Address, Location data, Name, Postal Code, Phone number, Photo	Health and Medical	Customer relationship, Administration, Compliance with law, Contract execution, Delivery Services, Vendor Management, Customer relationship, Administration, Compliance with law,	Regulatory Auditors	Life of Device + 2 years or life of contract +2 years	Contract Legal obligation

			Contract execution, Delivery Services, Vendor Management			
Others: End Customer Data Capture	Address, Country, Email, Location data, Postal Code, Name, Phone number, IP Address	N/A	Direct Marketing	3 rd Party Marketing Provider	Life of Device + 2 years or life of contract +2 years	Legitimate Interest Contract
Others Clinical Retinal Images	Photo Others: Could be personal information linked to image when provided	Biometric Data, Health and Medical, Vulnerable Persons (e.g. Children): It is possible to identify a young eye	Medical Research	External Reading Centers	Minimum of 6 years after each subject signed an authorization	Contract Legal obligation
Others Clinical Data for Medical Research	Date Of Birth Initials	Biometric Data, Health and Medical, Racial / Ethnic origin, Vulnerable Persons (e.g. Children), Religious / Philosophical beliefs:	Medical Research	Estenda External Grading by Experts Third Party Service Providers	minimum of 6 years after each subject signed an authorization	Contract Legal obligation Explicit Consent
Applicant Administration - Recruitment – Administration	Identification Data, Profession and employment, Personal Characteristics, Education and Training		Recruitment & Interview process Administration	HR Team Hiring Manager Recruitment Agency	2 Years (unsuccessful applicants) Perpetual for current employee, 6 years for post-employment.	Contract

Access and Badge Administration (Employee and Guest)	Identification data, Photo, Name, Job Title, Employee Number & Department (if applicable),		Security Management Insurance	IT Team HR Team Operations	Perpetual for current employee, Purged once a year for post-employment (Access)	Legitimate Interest
CCTV	Images of employees and visitors to UK sites	N/A	Protection of property & individuals on-site	Operations Team	CCTV UK cycle time – 2 weeks	Legitimate Interest